



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
ALAN@SMGIUSA.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE, LLC

Case No. 3:20sw110

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Carrie A Jarrett, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account: alan@smgiusa.com ("SUBJECT EMAIL ACCOUNT") that is stored at premises controlled by Google, LLC, (hereafter "Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California.
2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
3. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), currently assigned to the Richmond, Virginia Field Office. I have been a Special Agent since August 25,

2002. In the course of my duties, I am designated to investigate complex financial crimes, and more specifically, those violations that are related to federal fraud offenses.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of Title 18 U.S.C. Sections 1956(h) (conspiracy) and 1956(a)(2)(B) (money laundering) are presently located in the SUBJECT EMAIL ACCOUNT.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

RELEVANT STATUTORY PROVISIONS

7. **Conspiracy to Commit Money Laundering:** 18 U.S.C. § 1956(h) provides that any person who attempts or conspires to commit a money laundering offense shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the conspiracy.

8. **Money Laundering:** 18 U.S.C. § 1956(a)(2)(B) provides that it is unlawful for any person to transmit to the United States the proceeds of some form of unlawful activity knowing that the movement of the proceeds is designed to conceal the nature, location, source, ownership or control of the proceeds.

PROBABLE CAUSE

I. Relevant Individuals

9. Nitin Sandesara (“Sandesara”) is an Indian citizen, and Chairman of the Sandesara Group of companies, a diverse group of companies including Sterling Biotech Limited, PMT Machine Tools Limited, Sterling SEZ Limited, Sterling Ports Limited, Sterling International Enterprises Limited, and Sterling Oil Exploration & Energy Production Company Limited.

10. Dakshay Patel (“Dakshay”) is a naturalized United States citizen living in Chesterfield, Virginia. Dakshay’s home address is 14712 Green Summit Place in Colonial Heights (South Chesterfield), Virginia 23834. According to property records, Dakshay purchased this home for \$213,000 in or about October 1999. Dakshay is Sandesara’s brother-in-law.

11. Alan Moseley (“Moseley”) is a United States citizen employed by Sandesara and/or one of his associated companies, specifically SAIB, LLC.

II. Relevant Entities

12. Dakshay is associated with a number of Sandesara Group companies purportedly doing business in the United States.

13. For example, in or about May 2004, Dakshay registered the entity American Enterprises, LLC (“American Enterprises”) with the Virginia State Corporation Commission (“SCC”). According to the SCC, Dakshay was the sole member of American Enterprises, which intended to transact business as Sterling Gelatin. The address provided for American Enterprises, doing business as (“d/b/a”) Sterling Gelatin, was Dakshay’s home on Green Summit Place in Colonial Heights, Virginia.

14. Shortly thereafter, in or about 2005, Governor Mark Warner of Virginia announced that Sterling Gelatin, America, Inc. (“Sterling Gelatin”), a manufacturer of pharmaceutical gelatins, would invest \$2.5 million to build a distribution warehouse in Prince George County, Virginia. Governor Warner made the announcement following a meeting with company Chairman and Managing Director Nitin Sandesara (“Sandesara”), at Sterling Biotech, Ltd.’s¹ Mumbai, India headquarters. According to the press release, Dakshay (or “Danny” Patel) was the main point of contact for Sterling Gelatin in the United States.

15. In addition to Sterling Gelatin, Dakshay is the sole member of at least seven other companies associated with the Sandesara Group. These companies are purportedly based in Prince George, Virginia, within the Eastern District of Virginia. According to records filed with the Virginia SCC, six of these companies purport to engage in the following businesses among others: EagleAmerica, LLC (“EagleAmerica”) owns, operates, and maintains aircraft; Sterling Oil Resources, LLC (“Sterling Oil Resources”) engages in energy development; Virginia Star, LLC (“Virginia Star”) wholesales motor vehicle parts; and Washington Resources, LLC (“Washington Resources”) provides professional, scientific, and technical services.

16. Dakshay is also the sole member of SAIB, LLC (“SAIB”), which he incorporated in North Carolina on or about December 19, 2007. According to the Virginia SCC, SAIB engages in the business of leasing aircraft. Federal Aviation Administration (“FAA”) records indicated that a Model Gulfstream 200 aircraft, registration number N162GB, was first registered

¹ According to the Virginia Economic Development Partnership press release dated April 28, 2005, Sterling Biotech, Ltd. was the parent company of Sterling Gelatin, America, Inc.

to SAIB on or about March 7, 2008. Dakshay signed an Aircraft Registration Renewal Application for this aircraft late last year – on or about October 22, 2019.

17. Dakshay operates several other businesses in the Richmond Metro Region. Specifically, Dakshay operates, among other businesses, a restaurant, a motel, a gas station, a storage facility, and a convenience store under names such as Huddle House, Star Express, Sun Fuel, American Star, Sun Sub Tapp, American Eagle Self-Storage, American C-Stores, American Dync Holdings, and Sandesara Food Services.

III. Indian Criminal Charges

18. According to the Central Bureau of Investigation (CBI), in or about October 2017, the Enforcement Directorate of India (ED) charged Nitin Sandesara, his brother Chetan Sandesara, five other individuals, and 184 companies and shell companies, to include Sterling Biotech Limited, PMT Machine Tools Limited, Sterling SEZ Limited, Sterling Ports Limited, and Sterling Oil Exploration & Energy Production Company Limited with engaging in a conspiracy to defraud Indian banks of more than \$1 billion.

19. Records provided by the CBI alleged that Sandesara and his conspirators, through companies he controlled, submitted falsified documents to Indian banks in order to obtain loans, and he later used those same companies to divert the fraudulent proceeds.

20. The Times of India further reported on or about September 24, 2018:

It is alleged that the Sandesaras set up more than 300 shell companies in India and abroad which were used to divert loans. Officials said the modus operandi for money laundering used by the Sandesaras involved formation of shell[] companies, manipulating balance sheets, inflating turnover and insider shares trading. These firms were controlled by the Sandesaras through dummy directors, who were or are employees of various companies of the Sterling group. Bogus sales/purchases were shown between the [] companies and the Sterling group firms to divert loans and inflate turnover to obtain further loans from banks.

See <https://timesofindia.indiatimes.com/india/rs-5000-cr-bank-fraud-business-family-may-have-fled-to-nigeria/articleshow/65926859.cms>.

21. According to CBI records, the ED is also investigating Dakshay Patel as part of this case, as he was one of the Directors of Sterling Global Oil & Resources Pvt. Ltd.

22. In or about June 2019, the ED issued a provisional order under the Prevention of Money Laundering Act (PMLA) for attachment of property associated with the Sandesara Group including four oil rigs and an oil field in Nigeria, four Panama-registered ships, a residential flat in London, and a Gulfstream jet registered in the United States and owned by SAIB LLC, based in Prince George, Virginia.

23. The ED has not apprehended Sandesara or his brother, Chetan Sandesara. But FAA records indicate that the Gulfstream aircraft owned by SAIB completed numerous flights within Nigeria, a flight to the United States and between Nigeria and Albania from in or about August 2019 to the present. Additionally, Hitesh Kumar Patel, also Sandesara's brother, was detained pursuant to an Interpol Red Notice in or about March 2019 in Albania.

IV. Shell Companies and Front Companies

24. Dakshay currently maintains approximately 30 bank accounts at SONA Bank for the operation of his Richmond Metro Region businesses including a restaurant, a motel, a gas station, a storage facility, and a convenience store. Bank records for these businesses reflected revenue and operating expenses consistent with each specific type of business. That is, bank records included revenue and/or expenses involving the Virginia Lottery, batch credit card payments, Western Union charges, UHaul rentals, and fuel delivery. The bank accounts associated with the operation of these businesses did not contain any large monetary transactions,

nor any transfer of funds to bank accounts in the names of companies related to the Sandesara Group.

25. Dakshay also maintained at least ten additional bank accounts at various financial institutions over time in the names of companies related to the Sandesara Group, including EagleAmerica, SAIB, Sterling Oil Resources, Virginia Star, and Washington Resources.

26. All of these companies are purportedly located at 8700 Bull Hill Road or 4595 Sandesara Drive in Prince George, Virginia. These addresses are for the same location – a warehouse on the corner of Bull Hill Road and Sandesara Drive. Property records indicate that the 2.7 acres of land on which the warehouse is located and the warehouse itself is owned by Dakshay through an entity called Indus Holdings of Virginia, LLC. The signage on the warehouse reads “SMGI”, which according to Virginia SCC records, initially stood for Sandesara Management Group, Inc, but now stands for Sun Management Group, Inc. During surveillance of the location, there was no foot traffic seen going into or out of the warehouse. The inside was not visible through the windows as they were reflective.

27. The Virginia Employment Commission has no record of EagleAmerica, SAIB, Sterling Oil Resources, Virginia Star, and Washington Resources employing any individuals in the Commonwealth of Virginia.

28. Bank records for accounts in the names of these entities also do not reflect typical revenue or normal operating expenses, such as equipment purchases, inventory costs, research and development, marketing, payroll, and insurance.

29. The Virginia Department of Taxation also has no record of any state tax returns filed in 2017, 2018, and 2019 tax years for the following entities: EagleAmerica; SAIB; Sterling Oil Resources; Virginia Star; and Washington Resources. And the Internal Revenue Service

(“IRS”) has no record of any federal tax returns filed in 2016, 2017, and 2018 tax years for the following entities: EagleAmerica; Sterling Oil Resources; Virginia Star; and Washington Resources.

V. Monetary Transactions Involving Shell Companies

30. From in or about January 2017 through in or about September 2017, the following funds were wired to accounts held by Dakshay at Wells Fargo:

| | |
|------------------------|-----------------------------|
| \$19,719,840.00 | EagleAmerica, LLC |
| \$22,578,759.65 | Sterling Oil Resources, LLC |
| <u>\$ 2,005,000.00</u> | Virginia Star, LLC |
| \$44,303,599.65 | Total |

The \$44 million wired to these accounts was transmitted from entities outside the United States associated with Nitin Sandesara.

31. Moreover, the majority of funds deposited into these Wells Fargo accounts were later transferred back out of the United States to entities associated with Sandesara or transferred among the accounts held by Dakshay at Wells Fargo. These transactions usually occurred within one to three days of the initial wire transaction/deposit.

32. In or about September 2017, Wells Fargo Risk Management flagged a transaction involving an account ending in 7880 in the name of EagleAmerica, LLC. Dakshay was the sole signatory for this account.

33. That is, on or about September 6, 2017, the EagleAmerica account ending in 7880 received via wire transmission \$4,999,975 from the United Bank of Nigeria in the name of Sterling Oil Exploration and Energy, a company owned by Sandesara. The following day, on or about September 7, 2017, Dakshay wired \$5,061,234.88 from this same account to an account in the name of Nitin Sandesara at Hellenic Bank located in Cyprus.

34. Bank records indicate that Wells Fargo Risk Management contacted Dakshay about this transaction. Dakshay explained that he forwarded the \$5 million to the Chairman of the Board for a related company. Specifically, Dakshay stated that the funds were for a real estate purchase and needed to be seen coming from a U.S.-based bank account. Dakshay's explanation for the above-described transaction caused Wells Fargo employees to research the payee for the transferred funds – Nitin Sandesara. According to bank records, they determined Sandesara was part owner of the Sandesara Group of Companies and Sterling Biotech, Ltd., both of which were under investigation by India Enforcement Directorate for fraudulent bank schemes. Based on this information, on or about September 21, 2017, Wells Fargo decided to terminate its business relationship with Dakshay and his associated companies – American Enterprises, LLC; American Resources of Virginia, LLC; Washington Resources, LLC; American Eagle Self-Storage, LLC; Sterling Oil Resources, LLC; and Virginia Star, LLC.

35. Thereafter, Dakshay opened new bank accounts for these entities at BB&T Bank. Around this same time, EagleAmerica and Virginia Star obtained new employer identification numbers, which were submitted to BB&T Bank when accounts in the name of these entities were opened. That is, Dakshay opened a bank account in the name of Virginia Star in or about October 2017, and opened bank accounts in the name of EagleAmerica and Sterling Oil Resources in or about September 2018 and October 2018, respectively. Again, Dakshay was the sole signatory for these accounts.

36. From in or about October 2017 through in or about February 2019, the following funds were wired to accounts held by Dakshay at BB&T Bank:

| | |
|---------------------|-----------------------------|
| \$ 10,000 | EagleAmerica, LLC |
| \$ 1,000,000 | Sterling Oil Resources, LLC |
| <u>\$40,869,970</u> | Virginia Star, LLC |

\$41,879,970 Total

The \$41 million wired to these accounts was transmitted from entities outside the United States associated with Nitin Sandesara. Moreover, all of these funds were transmitted after the Enforcement Directorate of India charged Sandesara in or about October 2017 with a more than \$1 billion bank fraud conspiracy.

37. Dakshay transferred over \$28 million deposited in the Virginia Star bank account ending in 9223 to accounts in the name of 205 Capital LP at First Republic Bank in California. These accounts were controlled by Dakshay's relative Sunny Patel and Sandesara's nephew Yash Sandesara. Thereafter, at least \$22 million was transferred from 205 Capital accounts to purported investment funds and/or start-up businesses. However, more than half of these entities were inactive at the time the money was transferred from 205 Capital accounts, and remain inactive. Sunny and Yash also used more than \$5.6 million transferred to 205 Capital accounts for their own personal purposes, including rent and car payments.

38. On or about February 26, 2019, BB&T closed Dakshay's accounts in the name of Virginia Star, Sterling Oil Resources, and EagleAmerica based on a due diligence review by their law enforcement review team. According to bank records, BB&T closed the accounts because of activity indicative of money laundering. Specifically, BB&T was concerned about: (a) the receipt of wire transfer credits in round dollar amounts originating from a foreign jurisdiction; (b) that the transactions lacked a link to legitimate contracts, goods, or services and were inconsistent with Dakshay's stated line of business; (c) that the money was rapidly disbursed after received; and (d) that research by BB&T indicated Sterling Oil Resources, LLC was possibly linked to Nitin Sandesara, a fugitive economic offender wanted in India.

39. In or about November 2018, Dakshay transferred \$165,000 from Virginia Star's BB&T account to open a new account in the same name at Signature Bank. He also opened an account in the name of Sterling Oil Resources, LLC.

40. From in or about November 2018 through in or about May 2019 the following funds were received in accounts held by Dakshay at Signature Bank:

| | |
|---------------------|-----------------------------|
| \$ 200,000 | Sterling Oil Resources, LLC |
| <u>\$16,035,000</u> | Virginia Star, LLC |
| \$16,235,000 | Total |

The \$16 million wired to these accounts also was transmitted from entities outside the United States associated with Nitin Sandesara. Moreover, all of these funds were transmitted after the Enforcement Directorate of India charged Sandesara in or about October 2017 with a large-scale bank fraud conspiracy.

41. These bank accounts at Signature Bank include transactions similar to those in the earlier accounts maintained by Dakshay at Wells Fargo and BB&T. In or about May 2019, Dakshay closed the accounts at Signature Bank with a \$1,445,590.85 transfer from the Virginia Star account to Superflux Global Trading Co Ltd's bank account at Zenith Bank, PLC, 215B Etim Inyang Crescent, Victoria Island, Lagos. Dakshay also closed the Sterling Oil Resources, LLC account with a \$1,000 transfer to Cement Bond Nigeria Limited's account at Access Bank PLC, a Nigerian bank. Based on review of bank statements and information received from banking institutions, it appears all of Dakshay's personal and business accounts are currently at SONA Bank, a Virginia-based community bank.

42. From in or about June 2019 to the present, the following funds were received in accounts held by Dakshay at SONA Bank:

| | |
|----------------------|--------------------|
| \$4,232,903.54 | EagleAmerica, LLC |
| <u>\$ 700,000.00</u> | Virginia Star, LLC |
| \$4,932,903.54 | Total |

The nearly \$5 million wired to these accounts was transmitted from entities outside the United States associated with Nitin Sandesara. Moreover, all of these funds were transmitted after the Enforcement Directorate of India charged Sandesara in or about October 2017 with a large-scale bank fraud conspiracy.

43. The descriptions on the wire transmission forms that effected the above-described wire transmissions to accounts at Wells Fargo, BB&T, Signature Bank, and SONA Bank principally indicated the transactions were “payment for consultancy services.” In addition, the majority of the funds came from Nigerian-based banks. Wire transmissions were also received from Barbados, Vietnam, and Cyprus.

VI. SUBJECT EMAIL ACCOUNT Associated With Monetary Transactions

44. In or about May 2017, Dakshay contacted the FBI and reported that his company Sterling Oil Resources was the victim of a scam wherein they transferred \$3,785,275 in total via wire transmissions to the following specific entities based on fictitious email messages: Hawtai Technology CO, Ltd (\$520,287); Ezee B Resources (\$250,231); Homing Industrial Limited (\$800,213); Foshan Hongrui Trade Corporation (\$213,231); United Business Center Ltd (\$1,500,000); and Bismark Capital Sdn Bhd (\$501,313).

45. During an interview with FBI agents, Dakshay advised that he regularly used wire transmissions to conduct business internationally and the dollar amounts involved in the scam were not “out of the ordinary” for his business. Dakshay also noted four employees were involved in the process of completing a wire transfer for his business.

46. In his interview, Dakshay explained that he employed an account manager located in Prince George, Virginia who would receive requests for funds via email from the Chief Operating Officer of his company located in Nigeria, Africa. Dakshay stated that he received a copy of these emails, along with the Chairman of his company, Nitin Sandesara. These emails contained the destination financial institution, account number, and amount to be transferred. Sandesara typically approved the payment or transfer by sending a reply message via email to Dakshay and his Account Manager.

47. During this interview, Dakshay confirmed that his email account was danny@smgiusa.com. He further advised that his company used Google for their email accounts, and the domain for his U.S. operations was "smgiusa.com".

48. The internet domain for Dakshay's companies operating under Sun Management Group, Inc, is smgiusa.com. This domain was registered with Google, LLC by the company on or about July 10, 2010, and has been continuously owned by them since that time. According to analysis of the DNS² mail exchanger records, Google.com provides email services for all email addresses associated with the domain smgiusa.com, including the SUBJECT EMAIL ADDRESS – alan@smgiusa.com.

² "DNS" is an abbreviation for the Internet Domain Name System. DNS is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. In very short summary, two main functions provided by DNS servers are: 1) converting human readable communications using domain names (*e.g.*, email addresses, web addresses) to the numerical IP addresses needed for locating and identifying computer services and devices associated with those services; and 2) routing such communications to the correct IP address.

49. Dakshay also noted Sandesara and the Chief Operating Officer in Africa used “stoilmgt.com” as their domain. According to CentralOps.net, stoilmgt.com is a domain registered in Lagos, Nigeria, whose server is hosted by HostEurope GmbH, headquartered in Cologne, Germany.

50. On or about December 18, 2019, a federal Magistrate Judge in this Court found that there was probable cause to issue search warrants for email accounts associated with Dakshay Patel. Specifically, Google produced pursuant to these search warrants information associated with the email accounts: danny@smgiusa.com and ucpatel@smgiusa.com.

51. The contents of these email accounts included communications with Alan Moseley at alan@smgiusa.com as the principal point of contact regarding the Gulfstream aircraft registered to SAIB. That is, Moseley received and sent communications regarding the scheduling and payment of pilots, money transfers to Gulfstream Aerospace Corporation, Pratt & Whitney, LLC, and World Fuel Services, and general aircraft maintenance.

52. For example, on or about April 14, 2019, Moseley sent an email with the subject line, “Crew Changes” to Sandesara at chairman@stoilmgt.com and Dakshay at danny@smgiusa.com, that read in part: “I had to dismiss Dan Hopkins due to his attitude concerning the operations of the flight department, and using your name to inquire with his “outside contacts” in the FBI CIA. There have been other instances of violating proper company decorum.” Moseley also mentioned being in Abuja (the capital of Nigeria) providing coverage for the aircraft.

53. Shortly thereafter, on or about April 24, 2019, Moseley sent Sandesara and Dakshay an email about hiring aircraft crew; specifically, he stated that he was trying to hire people who could work out of Nigeria, had large aircraft experience, and an easy going

personality. The following day, Sandesara responded back to Moseley at alan@smgiusa.com:

“Dear Alan, Thanks. I don’t want anything different in a big way but in these turbulent times we stick to our trusted people. Regards, Nitin.”

54. On or about May 28, 2019, Moseley sent an email from alan@smgiusa.com to Sandesara regarding payments for aircraft crew. That is, Moseley informed Sandesara that unless the aircraft crew were paid they would be going home or ending their employment at the end of the week and upon arriving from Lagos to Abuja. That same day, Sandesara replied back to Moseley at alan@smgiusa.com:

There has been accounting and banking issue in USA office so no wire could take place. Danny and Banks are putting together new system in place which was to be operational last week but there is some delay.... It’s not a monetary issue at all but snags beyond our control.... Let me know if aircraft will be operational or not so that I can plan.

55. Information received from U.S. Customs and Border Protection Air and Marine Operations Center show from on or about August 7, 2019 through on or about November 11, 2019, tail number N162GB flew to the following locations: Munich, Germany; Zurich, Switzerland; Tirana, Albania; Hurgada, Egypt; Pristina, Kosova; and Abuja, Lagos, and Benin, Nigeria.

BACKGROUND CONCERNING EMAIL

56. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name smgiusa.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including

retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

57. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

58. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

59. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account

(including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

60. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

61. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such

as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

62. Generally, when served with a search warrant for electronic communications, the Internet service provider ("ISP"), such as Google, will send the contents of the specified account(s) to the investigating agency, usually on a CD or DVD, for the investigator to review. The ISP can copy the contents of the entire account because that is within their expertise. Though the ISP affirms that the records relate to the specified email account, the provider does not and will not undertake the examination of the contents of an account to make a determination as to what is relevant or irrelevant to the investigation. Generally, and in this case particularly,

the provider is not familiar with the investigation and is not in a position to identify the victim(s) or subject(s) of the investigation.

63. The provider is neither qualified nor trained to search the account information as would a law enforcement officer. Only a trained agent, familiar with the statutory violations and facts of the case, can determine what items should or should not be seized. For these reasons, I request the provider disclose the records listed in Section 1 of Attachment B, for the account(s) listed in Attachment A.

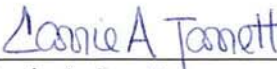
64. Based on what I know about the storage and deletion of email communications by a subscriber, I have requested by way of a preservation letter addressed to Google that data in the SUBJECT EMAIL ACCOUNT be maintained for the allowable 90 days which is due to expire June 21, 2020 with the expectation that a search warrant will be acquired for the production of such data.

CONCLUSION

65. Based on the forgoing, I respectfully submit that there is probable cause to believe that the SUBJECT EMAIL ACCOUNT, further described in Attachment A, contain evidence and instrumentalities of violations of Title 18, United States Code, Sections 1956(h) and 1956(a)(2)(B), further described in Attachment B.


66. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Carrie A. Jarrett
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 6th day of April, 2020.



/s/
Roderick C. Young
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with alan@smgiusa.com that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account January 1, 2017 to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18 U.S.C. Sections 1956(h) (conspiracy) and 1956(a)(2)(B) (money laundering) occurring between January 1, 2017 and present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence relating to the source of funds, requests and directions regarding movement of funds, both incoming and outgoing, where the funds are coming from, reason behind the transfer of funds, the ultimate disposition of funds and businesses involved in the transactions.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating state of mind of subjects as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

- (e) The identity of the person(s) who communicated with the user ID about matters relating to conspiracy, and money laundering, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney

communications to the investigative team. This investigation is presently covert and the government believes that the subject(s) of the search are not aware of the warrant.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, LLC, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, LLC, and they were made by Google, LLC as a regular practice; and

b. such records were generated by Google, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature